ABSTRACT OF THE DISCLOSURE

Methods and systems for encrypting and decrypting electronic files and then limiting the ability to copy, alter or send the decrypted information so as to preserve the integrity of the file. The encryption and decryption systems involve an essentially symmetric cipher or key system in which the same key is used to both encrypt the original plaintext and decrypt the resulting ciphertext. The key, or cipher, includes public and private components. The "public key" is typically stored and sent together with the encrypted file in the form of a unique file type that includes the public key appended to the front encrypted file portion. A new public key is typically generated for each electronic file that is encrypted. The "private key" is known only to the encrypting and decrypting parties and may be used to encrypt and decrypt multiple files, or it may be uniquely generated for each encrypted file. It may be hard-coded within the decryption software provided to the decrypting party, or it may be obtained by means of a secure password-protected login procedure. The software utilized in decrypting the encrypted file may also provide limited output, such as merely the ability to view and/or print a hard copy of the decrypted file.

G:\DATA\PAT\WORDPAT\15267.3.doc